NIAC
Vulnerability Disclosure Working Group (VDWG)

Final Report and Proposed Recommendations

John T. Chambers
President and CEO
Cisco Systems, Inc.

John W. Thompson
Chairman and CEO
Symantec Corporation

January 13, 2004

Presentation Outline

- Charter
- Methodology
- Findings
- Key Guidelines
- Conclusions
- Proposed Recommendations
- Next Steps
- Requests of the NIAC

Charter

- NIAC established Vulnerability Disclosure Working Group in December 2002
- Goals:
  - Develop global guidelines for handling security vulnerabilities from initial report to final resolution
  - Derive specific policy recommendations for the President
- This framework covers:
  - Notification
  - Investigation
  - Disclosure
  - Resolution

Methodology

- □ Formed inclusive Working Group representing all key stakeholder functions
- □ Conducted extensive literature search for best practices and white papers
- □ Surveyed WG members to further define problem and articulate stakeholder perspectives
- □ Developed key definitions and scope
- □ Wrote, reviewed, discussed
- □ Conducted two external reviews to ensure broad stakeholder representation
- □ Submitted final report to NIAC Members on Dec 19, 2003

Findings

- Framework requires common definitions
  - Vulnerability
  - Vulnerability life-cycle
  - Stakeholders
  - Scoring process
- Multiple perspectives are necessary; enrich solutions
- Communication is key to resolution; barriers exist
  - Inconsistent reporting procedures
  - Inconsistent use of encryption
  - Lack of assurance regarding protection of sensitive information
  - Confusion regarding authority of reports
- Legal landscape is complicated
  - Possible unintended consequences of privacy and security laws
  - Conflicting domestic and various national laws and regulations

Key Guidelines

- Definitions
  - Vulnerability
  - Vulnerability life-cycle
  - Stakeholders
- Stakeholders
  - Discoverers
  - Vendors
  - Users
  - Coordinators
- Communications
  - Suggestions for web sites
  - Suggestions for e-mail addresses
- Stakeholder roles and processes

Conclusions

1. Discoverers and vendors often disagree; but not regarding goal of improving security
2. Common terms and procedures are fundamental
3. Compatible encryption schemes are necessary
   - So all stakeholders can participate
   - To protect sensitive information

Conclusions (cont.)

4. Common threat scoring method may build common understanding
5. Robust information sharing is key to minimizing threats to critical infrastructure networks
6. Legal and regulatory frameworks at all levels need review to support secure sharing of vulnerability information

Proposed Recommendations

1. Support development of a common vulnerability management architecture
   - Common terms
   - Universally compatible procedures
   - Standardized e-mail addresses for reporting
   - Standardized web site locations and content

Proposed recommendations (cont.)

2. Provide trusted environments to protect vulnerability information and ongoing investigations

Proposed Recommendations (cont.)

3. Promote universal use of multiple compatible encryption methods
   - enables US Federal government to participate effectively in global vulnerability management process
   - compatible encryption benefits go beyond vulnerability management
   - key to improving communications

Proposed Recommendations (cont.)

4. Conduct a regulatory framework review

Proposed Recommendations (cont.)

5. Support robust voluntary information sharing through policy and funding. Set up or support neutral clearinghouses for vulnerability management

Proposed Recommendations (cont.)

6. Support a robust infrastructure for international coordination

Proposed Recommendations (cont.)

7. Promote and fund advanced university and industry security research and education

Next Steps

- NIAC approve report
- Threat scoring research task ongoing
  - Developing two-tiered methodology
  - First tier represents “base” or “raw” score
  - Second tier allows for site-specific or operational modification of base score
  - Weighted metrics and formula being developed
- Guidelines applicable to other NIAC working group efforts
- Need vehicle for updates

Requests of the NIAC

- Approve VDWG report
  - Discuss any changes and agree
  - Working group will make modifications as required
- Approve letter submitting report to President